US Government

Traffic Filter Firewall

Protection Profile

for

Low Risk Environments

Version 1.0

December 1997

Protection Profile Title:

US Government Traffic Filter Firewall Protection Profile for Low Risk Environments.

Criteria Version:

This Protection Profile (PP) was developed using the guidance, constructs, conventions, and requirements of Version 1.0 of the Common Criteria (CC) [1].

Constraints:

Targets of Evaluation (TOEs) developed to satisfy this Protection Profile shall be CC Part 2 Conformant and CC Part 3 Conformant.

Authors:

This Protection Profile was prepared by:

National Security Agency

Kris Britton
Jack Walsh

National Institute of Science and Technology

Wayne Jansen
Thomas Karygiannis

The Aerospace Corporation

Jandria Alexander
Mario Tinto

Acknowledgements:

The authors would like to acknowledge Ken Elliott (The Aerospace Corporation), Julie Connolly (MITRE Corporation), and reviewers of earlier drafts for their contributions.

Table of Contents

Conventions and Terminology

Conventions

The notation, formatting, and conventions used in this Protection Profile are consistent with those used in the Common Criteria, and with the example Protection Profiles of CCEB-96/014; "Part 4: Predefined Protection Profiles." Selected presentation choices are discussed here to aid the reader.

The Common Criteria allows several operations to be performed on functional requirements; *refinement, selection,* and *assignment,* defined in paragraph 2.1.2 of Part 2 (i.e., CCEB-96/012). Each of these operations are used in this Protection Profile.

> The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of functional requirements is denoted by **bold text**. For an example, see FIA_AFL.1 or FPT_TSA.2 of this Protection Profile.
>
> The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *underlined italicized text*. For an example, see FAU_MGT.1 of this Protection Profile
>
> The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [assignment_value]. For an example, see FDP_ACF.2 or FAU_SAR.3 of this Protection Profile.

As a vehicle for providing a further understanding of and context for functional requirements, "Requirements Overview" sections have been added to this Protection Profile. These overviews provide a discussion of the relationship between functional requirements so that the reader can see why a group of requirements were chosen and what effect they are expected to have as a group of related functions. As an example, see the Requirements Overview in paragraph 5.1.1 of this Protection Profile (describing the access control policy named in FDP_ACC.2).

Application Notes are provided to help the developer, either to clarify the intent of a requirement, identify implementation choices, or to define "pass-fail" criteria for a requirement. For example, see the application notes associated with FDP_RIP.3 of this Protection Profile.

Terminology

In the Common Criteria, the term *user* is defined as; "any entity (human or machine) outside the TOE that interacts with the TOE" (Part 1, Annex A). For the purpose of precision and clarity, the usage in this Protection Profile differs slightly from the definition of the Common Criteria. Specifically, for firewalls it is necessary to distinguish between interactions with which a human can be associated and those for which only a machine (e.g., a source address) is known. These terms are defined here.

User: A person outside the TOE that interacts with the TOE, and who has no special privileges that can effect the enforcement of the TOE Security Policy (TSP).

Authorized Administrator: Any authorized person that has privileges that can be used to bypass or circumvent the TSP. The term "authorized administrator" in this Protection Profile is meant to refer strictly to the administrator of the Firewall, and its use is not intended to include responsibilities for network administration.

Host: A machine outside the TOE that interacts with the TOE, and has no special privileges that can effect the enforcement of the TSP.

Trusted Host: Any authorized machine that has privileges that can be used to bypass or circumvent the TSP.

Document Organization

Section 1 is the introductory material for the Protection Profile

Section 2 provides a general definition for traffic filter firewalls.

Section 3 is a discussion of the expected environment for the firewall, in particular the assumptions that must be true about aspects such as physical, procedural, and administrative controls. This section then defines the policies that are supported by a compliant firewall, and the set of threats that are to be addressed by either the technical countermeasures implemented in the firewall's hardware and software, or through the environmental controls.

Section 4 defines the security objectives for both the firewall and the environment in which the firewall resides.

Section 5 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and Part 3, respectively, that must be satisfied by the firewall.

Section 6 provides a rationale for explicitly demonstrating that the set of requirements are complete relative to the objectives; that each security objective (e.g., O.ACCESS) is addressed by one or more relevant requirements.

Appendix A provides a list of relevant vulnerabilities against which PP compliant products must be checked.

Traffic Filter Firewall Protection Profile

1 INTRODUCTION

1.1 IDENTIFICATION

1 Title: US Government Traffic Filter Firewall Protection Profile for Low Risk Environments

2 Registration: <TBD>

3 Keywords: Access control, firewall, packet filter, network security, protection profile.

1.2 PROTECTION PROFILE OVERVIEW

4 This protection profile specifies the US government's minimum security requirements for traffic filtering firewalls used in low risk environments. The Protection Profile defines the threats that are to be addressed by the firewall, defines implementation-independent security objectives of the firewall and its environment, defines the functional and assurance requirements, and provides the rationale for the security objectives.

1.3 RELATED PROTECTION PROFILES:

5 US Government Application Level Firewall Protection Profile for Low Risk Environments [2]

2 TRAFFIC FILTER FIREWALL DESCRIPTION

6 The purpose of a firewall is to provide controlled and audited access to services, both from inside and outside an organization's private network by allowing, denying, and/or redirecting the flow of data through the firewall. Although there are a number of firewall architectures and technologies, firewalls basically fall into two major categories: traffic filters and application level gateways. This Protection Profile specifies the minimum requirements for traffic filtering firewalls. Figure 2.1

shows a logical representation of a firewall mediating access between internal and external networks.

7 Traffic filtering firewalls selectively route packets between internal and external networks according to a site's security policy. Traffic filtering decisions are typically made on the source address, destination address, protocol, source port, destination port, or are based on the interface the packet arrives or goes out on.

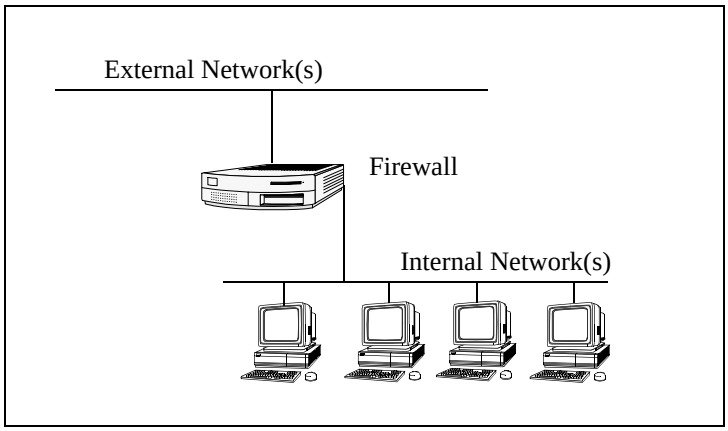

Figure 2.1 - Typical Firewall Location in Network

3 SECURITY ENVIRONMENT

8 PP-compliant products are intended for use in environments for which access control decisions based upon US DoD labeled information (i.e., multilevel information policies) are not supported. Thus, either the firewall will be used in environments in which, at most, sensitive but unclassified information is processed, or the sensitivity level of information in both the internal and external networks is the same. Firewalls compliant with this Protection Profile provide access control policies, Identification and Authentication (I&A), encryption of remote administrator sessions, some auditing capability, and a low level of assurance.

3.1 SECURE USAGE ASSUMPTIONS

9 The following conditions are assumed to exist in the operational environment.

A.SINGLEPT Single entry point

10 The firewall is the only interconnection point between networks, as shown in Figure 2.1.

A.SECURE Control of physical access

11 The firewall and associated directly-attached console is physically secure and available to authorized personnel only.

A.COMMS Protection of communications

12 The level of protection of any information transmitted is either consistent with the sensitivity of the information (e.g., via physically protected transmission media, encryption), or an explicit judgment has been made that the information may be transmitted as plaintext.

A.USER Users

13 The traffic filter firewall provides no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications). The firewall is essentially "transparent" to users. Only authorized administrators have direct access and may also have remote access.

A.NOEVIL Authorized administrators

14 Authorized administrators are assumed to be non-hostile, and trusted to perform their duties correctly.

3.2 THREATS TO SECURITY

15 This protection profile is sufficient for operational environments in which the threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low. The intent of the requirements is to provide the capability to control the flow of packets through the firewall in order to limit the ability of potentially malicious users from gaining access to the internal, protected network(s), or to specific hosts within the internal, protected network(s).

3.2.1 THREATS ADDRESSED BY THE FIREWALL

16 The threat possibilities discussed below are addressed by PP-compliant firewalls.

T.LACCESS Unauthorized logical access

17 An unauthorized person may gain logical access to the firewall. The term unauthorized person is used to cover all those persons who have, or may attempt to gain access to the system, but are not authorized users of the firewall.

T.ISPOOF Network address spoofing attacks

18 A subject may attempt to gain access to unauthorized information by masquerading as a different subject. For example, a subject on an external network may attempt to masquerade as a subject on an internal network by forging the network address of a valid, authorized internal subject.

T.NATTACK Attacks on the internal protected network

19 An attacker may attempt, usually by targeting high-level protocols and services, to attack the internal protected network or specific hosts within the internal protected network. Such attacks may be aimed at either denial of service or penetration of hosts or network nodes.

T.AUDIT Loss or Corruption of Audit Records

20 An attacker may be able to escape detection by taking actions that exhaust the audit storage capacity, thus causing audit records to be lost or destroyed.

T.DCORRUPT Modification of firewall configuration and/or other security-relevant data

21 This threat includes all attacks targeted against the firewall to read or modify firewall internal code or data structures, or to read or modify configuration and other security-relevant data (e.g., modify or destroy audit records).

T. AUTH Defeat of Identification and Authentication Mechanisms

22 An attacker may attempt to defeat or bypass the identification and authentication (I&A) mechanisms of the system in order to masquerade as a different, authorized administrator, or to intrude on an already established session. Examples of specific attacks are intercepting authentication information (e.g., passwords), replaying valid authentication exchanges, and session hijacking.

3.2.2 THREATS TO BE ADDRESSED BY OPERATING ENVIRONMENT

23 The threat possibilities discussed below must either be countered by physical controls, procedural measures, or administrative methods.

T.INSHARE Hostile users on a protected network (“inside” the firewall) attempting to give information to users on an external network

24 This threat deals with the case that a user on an internal (protected) network attempts to send information to an unauthorized user on an external network. Since

firewalls are basically designed to protect internal networks from external networks, they will be generally ineffective against these kinds of threats.

T.INALL Hostile users on a protected network attack machines also on the protected network

25 Because a firewall by design is primarily to protect users on a network "inside" the firewall from users external to the firewall, it cannot control traffic that does not cross the firewall. Attacks falling in this category come from attacks on network services originating within the protected network, and targeting machines on that same network segment.

T.SERVICES Attacks on higher-level protocols and services

26 These types of attacks target bugs in protocol layers (and services using those protocols, e.g., HTTP) above the transport layer. PP-compliant firewalls may be able to completely deny access to specific hosts or groups of hosts, but if packets are allowed to pass, then attacks on the services they are targeted for are possible.

T.PRIVACY Interception of transmitted information

27 An attacker may intercept sensitive information transmitted through the firewall.

4 SECURITY OBJECTIVES

4.1 INFORMATION TECHNOLOGY (IT) SECURITY OBJECTIVES

28 The following are the IT security objectives for the firewall:

O.ACCESS Access Mediation

29 The objective is to provide controlled access between networks connected to the firewall by permitting or denying the flow of information from a subject (sending entity) to an object (receiving entity) based on the attributes of the subject, object, and administratively configured access control rules.

O.ADMIN Administrator Access

30 This objective seeks to limit access to the firewall to authorised, administrative personnel, and to give only those individuals the ability to configure and administer the firewall.

O.ACCOUNT Individual Accountability

31 This objective seeks to provide user accountability, and allows access decisions to be made based on a unique identity. Authentication provides a means to establish the validity of the claimed identity.

O.PROTECT Firewall Self-Protection

32 In order to successfully meet this objective, the firewall must be able to separate data that it needs to operate from data that it is processing. It must protect itself from attacks by external entities. As a related issue, the firewall must be capable of protecting communications sessions of authorized administrators.

O.AUDIT Auditing

33 An audit trail is vital to determining if there are on-going attempts to circumvent the security policy, or if there are mis-configurations of the firewall that unwittingly allow access where it should be denied. Not only must the audit data be collected, but it must be viewable and relatively easy to work with. Finally, the audit trail must be sufficiently protected and the scope of potential audit record loss known so that sound security decisions by an authorized administrator can be supported.

4.2 NON-IT SECURITY OBJECTIVES

34 These are the objectives that are to be satisfied without imposing technical requirements on the firewall. That is they will not require implementation of mechanisms in the firewall hardware and/or software. Thus, they will be satisfied largely through application of physical, procedural, or administrative measures.

35 The following are the PP non-IT security objectives:

O.INSTALL Installation and Operational Controls

36 This objective is aimed at ensuring that the firewall is delivered, installed, managed and operated in a manner which maintains the system security.

O.PACCESS Physical Controls

37 Physical access to the firewall is controlled.

O.TRAIN Authorized Administrator Training

38 Authorized administrators are trained as to establishment and maintenance of sound security policies and practices.

5 IT SECURITY REQUIREMENTS

5.1 FIREWALL IT SECURITY REQUIREMENTS

39 This section provides functional and assurance requirements that must be satisfied by a PP-compliant firewall. These requirements consist of functional components from Part 2 of the CC and an Evaluation Assurance Level (EAL) containing assurance components from Part 3.

5.1.1 FUNCTIONAL REQUIREMENTS

40 The functional security requirements for this PP consist of the following components from Part 2, summarized in the following table:

Functional Class	Functional Components	
User Data Protection	FDP_ACC.2	Complete Object Access Control
	FDP_ACF.4	Access Authorization and Denial
	FDP_ACF.2	Multiple Security Attribute Access Control
	FDP_RIP.3	Full Residual Information Protection on Allocation
	FDP_SAM.1	Administrator Attribute Modification
	FDP_SAQ.1	Administrator Attribute Query

Table 5.1 - Functional Requirements

Identification and Authentication	FIA_ADA.1	**Authorized Administrator and Trusted Host** Authentication Data Initialization
	FIA_ADP.1	Basic **Authorized Administrator and Trusted Host** Authentication Data Protection
	FIA_AFL.1	Basic Authentication Failure Handling
	FIA_ATA.1	**Authorized Administrator, Trusted Host, and Host** Attribute Initialization
	FIA_ATD.2	Unique **Authorized Administrator, Trusted Host, and Host** Attribute Definition
	FIA_UAU.1	Basic **Authorized Administrator** Authentication
	FIA_UAU.2	Single-use Authentication Mechanisms
	FIA_UID.2	Unique Identification of **Authorized Administrators, Trusted Hosts, and Hosts**
Cryptographic Support	FCS_COP.2	Standards-Based Cryptographic Operation
Protection of the Trusted Security Functions	FPT_RVM.1	Non-Bypassability of the TSP
	FPT_SEP.1	TSF Domain Separation
	FPT_TSA.2	Separate Security Administrative Role
	FPT_TSM.1	Management Functions
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_MGT.1	Audit Trail Management
	FAU_POP.1	Human Understandable Format
	FAU_PRO.1	Restricted Audit Trail Access
	FAU_SAR.1	Restricted Audit Review
	FAU_SAR.3	Selectable Audit Review
	FAU_STG.3	Prevention of Audit Data Loss

Table 5.1 - Functional Requirements

Requirements Overview:The TSP is made up of one Security Function Policy (SFP). The policy is defined below. The policy, called UNAUTHENTICATED_END-TO-END_POLICY, deals with subjects on an internal or external network sending traffic through the TOE to objects on an external or internal network.

FDP_ACC.2 Complete Object Access Control

41 FDP_ACC.2.1 The TSF shall enforce the [UNAUTHENTICATED_END-TO-END_POLICY], on:

a) [The subjects: hosts not authenticated at the TOE].

b) [The objects: hosts on the internal or external network(s)].

[and all operations among subjects and objects covered by the Security Function Policy (SFP)].

42 FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by the SFP.

FDP_ACF.4 Access Authorization and Denial

43 FDP_ACF.4.1 The TSF shall enforce the:

- [UNAUTHENTICATED_END-TO-END_POLICY]

to provide the ability to explicitly grant access based on the value of security attributes of subjects and objects.

44 FDP_ACF.4.2 The TSF shall enforce the:

- [UNAUTHENTICATED_END-TO-END_POLICY]

to provide the ability to explicitly deny access based on the value of security attributes of subjects and objects.

FDP_ACF.2 Multiple Security Attribute Access Control

45 FDP_ACF.2.1 The TSF shall enforce the:

- [UNAUTHENTICATED_END-TO-END_POLICY],

to objects based on [source address, destination address, transport layer protocol, and service requested (e.g., source port number and/or destination port number)].

46 FDP_ACF.2.2 The TSF shall enforce the following **additional** rules to determine if an operation among controlled subjects and controlled objects is allowed:

a) [The TOE shall reject requests for access or services that originate from an external, unprotected network, but which have the source address of a host on an internal, protected network];

b) [The TOE shall reject requests for access or services that originate from an external, unprotected network, but which have the source address of a broadcast network];

c) [The TOE shall reject requests for access or services that originate from an external, unprotected network, but which have the source address of a host on a private, reserved network];

d) [The TOE shall reject requests for access or services that originate from an external, unprotected network, but which have the source address of a host on the loopback network].

FDP_RIP.3 Full Residual Information Protection on Allocation.

47 FDP_RIP.3.1 The TSF shall ensure that upon the allocation of a resource to all objects any previous information content is unavailable.

Application Note: This requirement deals with the need to manage all resources (e.g., registers, buffers) used to support connections such that access to information from previous sessions is not permitted. This requirement is usually satisfied via clearing or overwriting such resources.

Requirements Overview:The next two requirements (i.e., FDP_SAM.1, FDP_SAQ.1) identify the capabilities required to support the administrator role, specifically the capability to review and modify security-related attributes. These are elaborated on or augmented in the following requirements that deal with the need for the TOE to support the initialization of several security-related data.

FDP_SAM.1 Administrator Attribute Modification

48 FDP_SAM.1.1 The TSF shall enforce the *access control SFP:*

- *UNAUTHENTICATED_END-TO-END_POLICY*

to provide authorized administrators with the ability to modify:

- [The association of IDs with roles (e.g., authorized administrator)];
- [access control attributes identified in FDP_ACF.2];
- [security relevant administrative data].

FDP_SAQ.1 Administrator Attribute Query

49 FDP_SAQ.1.1 The TSF shall enforce the *access control SFP:*

- *UNAUTHENTICATED_END-TO-END_POLICY*

to provide the authorized administrator with the ability to query:

- [access control attributes identified in FDP_ACF.2];
- [host names].

FIA_ADA.1 **Authorized Administrator and Trusted Host** Authentication Data Initialization

50 FIA_ADA.1.1 The TSF shall provide functions for initializing **authorized administrator and trusted host** authentication data related to [authentication mechanisms identified in FIA_UAU.1 and FIA_UAU.2].

51 FIA_ADA.1.2 The TSF shall restrict use of these functions to the authorized administrator.

FIA_ADP.1 Basic **Authorized Administrator and Trusted Host** Authentication Data Protection

52 FIA_ADP.1.1 The TSF shall protect from unauthorized observation, modification, and destruction authentication data that is stored in the TOE.

FIA_AFL.1 Basic Authentication Failure Handling

53 FIA_AFL.1.1 The TSF shall be able to terminate **a trusted host** session establishment process after **[a settable number] of** unsuccessful authentication attempts. **The failure threshold shall be settable only by an authorized administrator.**

54 FIA_AFL.1.2 After the termination of **a trusted host** session establishment process the TSF shall be able to disable the ***trusted host account*** until [the session is unblocked by an authorized administrator].

FIA_ATA.1 **Authorized Administrator, Trusted Host, and Host** Attribute Initialization

55 FIA_ATA.1.1 The TSF shall provide the ability to initialize **authorized administrator, trusted host, and host** attributes with provided default values.

FIA_ATD.2 Unique **Authorized Administrator, Trusted Host, and Host** Attribute Definition

56 FIA_ATD.2.1 The TSF shall provide, **for each authorized administrator, trusted host, and host that is defined to it**, a unique set of security attributes necessary to enforce the TSP.

FIA_UAU.1 Basic **Authorized Administrator** Authentication

57 FIA_UAU.1.1 The TSF shall authenticate any **authorized administrator's** claimed identity prior to performing any functions for the **authorized administrator when the authorized administrator accesses the TOE through the console**.

FIA_UAU.2 Single-use Authentication Mechanisms

58 FIA_UAU.2.1 The TSF shall authenticate any **authorized administrator's or trusted host's** claimed identity prior to performing any functions for the **corresponding authorized administrator or trusted host**.

59 FIA_UAU.2.2 The TSF shall prevent reuse of authentication data related to [remote administration, and remote trusted host operation].

FIA_UID.2 Unique Identification of **Authorized Administrators, Trusted Hosts, and Hosts**

60 FIA_UID.2.1 The TSF shall uniquely identify each **authorized administrator, trusted host, or host** before performing any actions requested by the **corresponding authorized administrator, trusted host, or host**.

FCS_COP.2 Standards-Based Cryptographic Operation

61 FCS_COP.2.1 The TSF shall perform [encryption of remote administration sessions, compliant with FIPS 140-1 [3] in accordance with a specified cryptographic algorithm and cryptographic key size which meet the following standard: [FIPS 46-2 and 81: Data Encryption Standard (DES) and DES Modes of Operation [4], [5]].

Requirements Overview:The next two requirements (i.e., FPT_RVM.1 and FPT_SEP.1) deal with the fundamental architectural ability to protect its internal code and data structures, and to be able to demonstrate that the security policy is always invoked.

FPT_RVM.1 Non-Bypassability of the TSP

62 FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before any security-related operation is allowed to proceed.

FPT_SEP.1 TSF Domain Separation

63 FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

64 FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Application Note: TOEs meeting this PP do not need to satisfy FPT_SEP.1.2.

FPT_TSA.2 Separate Security Administrative Role

65 FPT_TSA.2.1 The TSF shall distinguish security-relevant administrative functions from other functions.

66 FPT_TSA.2.2 The TSF's set of security-relevant administrative functions shall include all functions necessary to install, configure, and manage the TSF; minimally, this set shall include [add and delete subjects and objects; view security attributes; assign, alter, and revoke security attributes; review and manage audit data].

67 FPT_TSA.2.3 The TSF shall restrict the ability to perform security-relevant administrative functions to a security administrative role that has a specific set of authorized functions and responsibilities.

68 FPT_TSA.2.4 The TSF shall be capable of distinguishing the set of **authorized administrators and trusted hosts** authorized for administrative functions from the set of all **individuals and systems using** the TOE.

69 FPT_TSA.2.5 The TSF shall allow only **authorized administrators and trusted hosts** to assume the security administrative role.

70 FPT_TSA.2.6 The TSF shall require an explicit request to be made in order for an **authorized administrator or trusted host** to assume the security administrative role.

FPT_TSM.1 Management Functions

71 FPT_TSM.1.1 The TSF shall provide the authorized administrator with the ability to set and update [security relevant administrative data].

72 FPT_TSM.1.2 The TSF shall provide the authorized administrator with the ability to perform [installation and initial configuration of the TOE; functions that allow system start-up and shutdown; backup and recovery]. **The backup capability shall be supported by automated tools.**

73 **If the TSF supports remote administration from either the internal or external interface, the TSF shall:**

a) Have the option of disabling remote administration on either the internal, external, or both interfaces.

b) Be capable of restricting the address from which remote administration can be performed.

c) Be capable of protecting the remote administration dialogue through encryption.

Requirements Overview: The remaining functional security requirements (Class FAU) deal with the need for producing, managing, protecting, and processing security audit information.

FAU_GEN.1 Audit Data Generation

74 FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions.

b) All auditable events **relevant** for the *basic* level of audit defined in **those** functional components **specified in Table 5.2** in the PP/ST.

c) Based on all functional components included in the PP/ST, *additional event(s) indicated as "extended" in Table 5.2*.

75 FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity and *success or failure* of the event.

b) **Additional information specified in column four of Table 5.2** for each audit event type, based on the auditable event definitions of the other

functional components included in the Protection Profile and/or Security Target.

Parent Family	Level	Auditable event	Additional Audit Record Contents
FAU_MGT	basic	Any attempt to perform an operation on the audit trail, including shutdown of the audit functions/subsystem.	Object ID of the audit trail object affected, if applicable.
FAU_PRO	basic	Any attempt to read, modify or destroy the audit trail.	
FDP_ACF	basic	All requests to perform an operation on an object covered by the SFP.	The object ID of the affected object.
FDP_SAM	basic	All attempts to modify security attributes, including the identity of the target of the modification attempt.	The new values of the modified security attributes.
FIA_ADA	basic	All requests to use TSF authentication data management mechanisms.	
FIA_ADP	basic	All requests to access authentication data.	The target of the access request.
FIA_AFL	extended	The termination of a session caused by a number of unsuccessful authentication attempts that exceed the threshold setting.	The identifier used.
FIA_UAU	basic	Any use of the authentication mechanism.	
FIA_UID	basic	All attempts to use the identification mechanism, including identity provided.	
FPT_TSM	basic	Successful and unsuccessful attempts to modify (set and update) TSF configuration parameters.	The new values of the configuration parameters.

Table 5.2 - Auditable Events

FAU_MGT.1 Audit Trail Management

76 FAU_MGT.1.1 The TSF shall provide the authorized administrator with the ability to *create, archive, delete, and empty* the audit trail.

FAU_POP.1 Human Understandable Format

77 FAU_POP.1.1The TSF shall provide the capability to generate human understandable presentation of any audit data stored in the permanent audit trail.

FAU_PRO.1 Restricted Audit Trail Access

78 FAU_PRO.1.1 The TSF shall restrict access to the audit trail to the authorized administrator.

FAU_SAR.1 Restricted Audit Review

79 FAU_SAR.1.1 The TSF shall provide audit review tools, with the ability to view the audit data.

80 FAU_SAR.1.2 The TOE shall restrict the use of the audit review tools to the authorized administrator.

FAU_SAR.3 Selectable Audit Review

81 FAU_SAR.3.1 The TSF shall provide audit review tools with the ability to perform searches and sorting of audit data based on:

- [Subject ID;
- Object ID;
- Date;
- Time;
- And logical (e.g., AND, OR) combinations of the above parameters]

Application Note: The author of the Security Target (ST) is expected to describe the detailed capabilities of the audit review tools. In particular, the ability to search and sort based on security-relevant attributes must be described.

FAU_STG.3 Prevention of Audit Data Loss

82 FAU_STG.3.1 The TSF shall store generated records of audit in a permanent audit trail.

83 FAU_STG.3.2 The TSF shall limit the number of audit events lost due to *failure and attack*.

84 FAU_STG.3.3 In the event of audit storage exhaustion, the TSF shall be capable of *preventing* the occurrence of auditable actions, except those taken by the authorized administrator.

Application Note: It is expected that the TOE developer will provide an analysis of the maximum amount of audit data that can be expected to be lost resulting from failure or audit storage exhaustion.

5.1.2 ASSURANCE REQUIREMENTS

85 The assurance requirements levied on the developer consist of EAL2 and are summarized in the following table.

Assurance Class	Assurance Components	
Configuration Management	ACM_CAP.1	Minimal Support
Delivery and Operation	ADO_IGS.1	Installation, Generation, and Start-up Procedures
Development	ADV_FSP.1	TOE and Security Policy
	ADV_HLD.1	Descriptive High-Level Design
	ADV_RCR.1	Informal Correspondence Demonstration
Guidance Documents	AGD_ADM.1	Administrator Guidance
	AGD_USR.1	User Guidance
Tests	ATE_IND.1	Independent Testing - Conformance
	ATE_COV.1	Complete Coverage - Informal
	ATE_FUN.1	Functional Testing
	ATE_DPT.1	Testing - Functional Specification
Vulnerability Analysis	AVA_SOF.1	Strength of TOE Security Function Evaluation
	AVA_VLA.1	Developer Vulnerability Analysis

Table 5.3 - Assurance Requirements; EAL2

ACM_CAP.1 Minimal Support

86 ACM_CAP.1.1D The developer shall use a configuration management (CM) system.

87 ACM_CAP.2D The developer shall provide CM documentation.

88 ACM_CAP.1C The CM documentation shall include a configuration list.

89 ACM_CAP.2C The configuration list shall describe the configuration items that comprise the TOE, **and shall include the external network services that are used by the TOE**.

90 ACM_CAP.3C The CM documentation shall describe the method used to uniquely identify the TOE configuration items.

91 ACM_CAP.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1 Installation, Generation, and Start-up Procedures

92 ADO_IGS.1.1.D The developer shall document procedures to be used for the secure installation, generation, and start-up of the TOE.

93 ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

94 ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1 TOE and Security Policy

95 ADV_FSP.1.1D The developer shall provide a functional specification.

96 ADV_FSP.1.2D The developer shall provide a TSP.

97 ADV_FSP.1.1C The functional specification shall describe the TSP using an informal style.

98 ADV_FSP.1.2C The functional specification shall include an informal presentation of syntax and semantics of all external TSF interfaces.

99 ADV_FSP.1.3C The functional specification shall include evidence that demonstrates that the TSF is completely represented.

Application Note: This requirement potentially can be met by a combination of documents, including the Security Target and external interface specification.

100 ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

101 ADV_FSP.1.2E The evaluator shall determine that the functional specification is consistent with the TSP.

102 ADV_FSP.1.3E The evaluator shall determine if the functional requirements in the Security Target are addressed by the representation of the TSFs.

ADV_HLD.1 Descriptive High-Level Design

103 ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

104 ADV_HLD.1.1C The presentation of the high-level design shall be informal.

105 ADV_HLD.1.2C The high-level design shall describe the structure of the TSF in terms of subsystems.

106 ADV_HLD.1.3C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

107 ADV_HLD.1.4C The high-level design shall identify the interfaces of the subsystems of the TSF.

108 ADV_HLD.1.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

109 ADV_HLD.1.1E The evaluator shall conform that the information provided meets all requirements for content and presentation.

110 ADV_HLD.1.2E The evaluator shall determine if the functional requirements in the ST are addressed by the representation of the TSF.

ADV_RCR.1 Informal Correspondence Demonstration

111 ADV_RCR.1.1D The developer shall provide evidence that the least abstract TSF representation provided is an accurate, consistent, and complete instantiation of the functional requirements expressed in the ST.

112 ADV_RCR.1.1C For each adjacent pair of TSF representations, the evidence shall demonstrate that all parts of the more abstract representation are refined in the less abstract representation.

113 ADV_RCR.1.2C For each adjacent pair of TSF representations, the demonstration of correspondence between the representations may be informal.

114 ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

115 ADV_RCR.1.2E The evaluator shall analyze the correspondence between the functional requirements expressed in the ST and the least abstract representation provided to ensure accuracy, consistency, and completeness.

AGD_ADM.1 Administrator Guidance

116 AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

117 AGD_ADM.1.1C The administrator guidance shall describe how to administer the TOE in a secure manner.

118 AGD_ADM.1.2C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

119 AGD_ADM.1.3C The administrator guidance shall contain guidelines on the consistent and effective use of the security functions within the TSF.

120 AGD_ADM.1.4C The administrator guidance shall describe the difference between two types of functions: those which allow an administrator to control security parameters, and those which allow the administrator to obtain information only.

121 AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the administrator's control.

122 AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

123 AGD_ADM.1.7C The administrator guidance shall contain guidelines on how the security functions interact.

124 AGD_ADM.1.8C The administrator guidance shall contain instructions regarding how to configure the TOE.

125 AGD_ADM.1.9C The administrator guidance shall describe all configuration options that may be used during secure installation of the TOE.

126 AGD_ADM.1.10C The administrator guidance shall describe details, sufficient for use, of procedures relevant to the administration of security.

127 AGD_ADM.1.11C The administrator guidance shall be consistent with all other documents supplied for evaluation.

128 AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

129 AGD_ADM.1.2E The evaluator shall confirm that the installation procedures result in a secure configuration

Application Note: This requirement is expected to be satisfied through meeting AGD_ADM.1.

AGD_USR.1 User Guidance

130 AGD_USR.1.1D The developer shall provide user guidance.

131 AGD_USR.1.1C The user guidance shall describe the TSF and interfaces available to the user.

132 AGD_USR.1.2C The user guidance shall contain guidelines on the use of security functions provided by the TOE.

133 AGD_USR.1.3C The user guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

134 AGD_USR.1.4C The user guidance shall describe the interaction between user-visible security functions.

135 AGD_USR.1.5C The user guidance shall be consistent with all other documentation delivered for evaluation.

136 AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1 Independent Testing - Conformance

137 ATE_IND.1.1D The developer shall provide the firewall for testing.

138 ATE_IND.1.1C The firewall shall be suitable for testing.

139 ATE_IND.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_COV.1 Complete Coverage - Informal

140 ATE_COV.1.1D The developer shall provide an analysis of the test coverage.

141 ATE_COV.1.1C The analysis of the test coverage shall demonstrate that the tests identified in the test documentation cover the TSF.

142 ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 Functional Testing

143 ATE_FUN.1.1D The developer shall test the TSF and document the results.

144 ATE_FUN.1.2D The developer shall provide test documentation.

145 ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, and test results.

146 ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

147 ATE_FUN1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function.

148 ATE_FUN.1.4C The test results in the test documentation shall show the expected results of each test

149 ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each security function operates as specified.

150 ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_DPT.1 Testing - Functional Specification

151 ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

152 ATE_DPT.1.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TOE operates in accordance with the functional specification of the TSF.

153 ATE_DPT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1 Strength of the TOE Security Function Evaluation[1]

154 AVA_SOF.1.1D The developer shall identify all TOE security mechanisms for which a strength of TOE security function analysis is appropriate.

155 AVA_SOF.1.2D The developer shall perform a strength of TOE security function analysis for each identified mechanism. **FIA_UAU mechanisms shall meet the random number generation tests in FIPS-PUB 140-1, Section 4.11.1, "Statistical Random Number Generation Test" (pg. 32 - 33).**

156 AVA_SOF.1.1C The strength of TOE security function analysis shall determine the impact of the identified TOE security mechanisms on the ability of the TOE security functions to counter the threats.

157 AVA_SOF.1.2C The strength of TOE security function analysis shall demonstrate that the identified strength of the security functions is consistent with the security objectives of the TOE.

158 AVA_SOF.1.3C Each strength claim shall be either **medium or high**.[2]

159 AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

160 AVA_SOF.1.2E The evaluator shall confirm that all TOE security mechanisms requiring a strength analysis have been identified.

161 AVA_SOF.1.3E The evaluator shall confirm that the strength claims are confirmed.

Application Note: The analysis and testing of the random number generator is fundamental to the kinds of mechanisms for which AVA_SOF is applicable. However, compliance with the Statistical Random Number Generation Test in FIPS 140-1 is necessary, but not sufficient for demonstrating that a given mechanism satisfies the requirements. It must also be shown that the algorithm for generating, using, and exchanging secrets, as well as the strength of the associations (e.g., association of a password with a person or host) is adequate. Thus, the developer must show—and the evaluator perform the requisite analysis—that the overall design and implementation of the mechanism is sufficient for meeting the requirements of the firewall (e.g., strength of authentication).

1. AVA_SOF is intended to apply strictly to those security mechanisms that are amenable to attack as a result of quantitative or statistical analysis (e.g., passwords). A fuller discussion is provided in the Part 3 of the CC, in AVA_SOF, "Objectives."

AVA_VLA.1 Developer Vulnerability Analysis

162 AVA_VLA.1.1D The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP. **This search shall include, but is not limited to, a search for vulnerabilities identified in Appendix A.**

163 AVA_VLA1.2D The developer shall document the disposition of identified vulnerabilities.

164 AVA_VLA.1.1C The evidence shall show, for each vulnerability, that the vulnerability cannot be exploited in the intended environment for the TOE.

165 AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

166 AVA_VLA.1.2E The evaluator shall conduct penetration testing, based on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6 RATIONALE

6.1 RATIONALE FOR IT SECURITY OBJECTIVES

O.ACCESS Access Mediation

167 This security objective is necessary to counter threats T.ISPOOF, T.NATTACK, and T.DCORRUPT.

O.ADMIN Administrator Access

168 This security objective is necessary to counter threats T.LACCESS, T.ISPOOF, and T.DCORRUPT.

O.ACCOUNT Individual Accountability

169 This security objective is necessary to counter threat T.LACCESS.

2. The definitions of "medium" and "high" are given in Part 3 of the CC under AVA_SOF, "Application Notes."

O.PROTECT Firewall Self-Protection

170 This security objective is necessary to counter threats T.DCORRUPT and T.AUTH.

O.AUDIT Auditing

171 This security objective is necessary to counter threats T.NATTACK, T.AUDIT, and T.DCORRUPT.

	O.ACCESS	O.ADMIN	O.ACCOUNT	O.PROTECT	O.AUDIT
T.LACCESS		X	X		
T.ISPOOF	X	X			
T.NATTACK	X				X
T.AUDIT					X
T.DCORRUPT	X	X		X	X
T.AUTH				X	

Table 6.1 - Summary of Mappings Between Threats and IT Security Objectives

6.2 RATIONALE FOR NON-IT SECURITY OBJECTIVES

O.INSTALL Installation and Operational Controls

172 This security objective is necessary to counter threats T.LACCESS, T.ISPOOF, T.NATTACK, T.AUDIT, T.DCORRUPT, and T.AUTH.

O.PACCESS Physical Controls

173 This security objective is necessary to counter threats T.ISPOOF, T.NATTACK, and T.DCORRUPT.

O.TRAIN Authorized Administrator Training

174 This security objective is necessary to counter threats T.LACCESS, T.ISPOOF, T.NATTACK, T.AUDIT, T.DCORRUPT, and T.AUTH.

	O.INSTALL	O.PACCESS	O.TRAIN
T.LACCESS	X		X
T.ISPOOF	X	X	X
T.NATTACK	X	X	X
T.AUDIT	X		X
T.DCORRUPT	X	X	X
T.AUTH	X		X

Table 6.2 - Summary of Mappings Between Threats and IT Security Objectives

6.3 RATIONALE FOR IT FUNCTIONAL REQUIREMENTS

FDP_ACC.2 Complete Object Access Control

175 This component was chosen to provide the basic definitions for the access control functionality of the firewall. This component directly supports the Access Mediation security objective, O.ACCESS.

FDP_ACF.4 Access Authorization and Denial

176 This component was chosen to require the ability to configure the access control functionality of the firewall; this actually allows the administrator to implement the policy. This component directly supports the Access Mediation security objective, O.ACCESS.

FDP_ACF.2 Multiple Security Attribute Access Control

177 This component was chosen to provide the access control functionality of the firewall. This component directly supports the Access Mediation security objective, O.ACCESS.

FDP_RIP.3 Full Residual Information Protection on Allocation

178 This component was chosen to avoid exposure of residual data in storage objects. This component supports the access control policy by guaranteeing that users do not

accidentally acquire data not explicitly granted to them. This component supports O.ACCESS.

FDP_SAM.1 Minimal Attribute Modification

179 This component was chosen to require that administrators be the only ones to have the ability to configure the access control functionality of the firewall. These are the only "attributes" that can be modified by administrators of the firewall. This component directly supports the Access Mediation security objective, O.ACCESS. This component also supports the Administrator Access security objective, O.ADMIN.

FDP_SAQ.1 Minimal Attribute Query

180 This component was chosen to allow the administrators the ability to view the access control rules they set up. This component directly supports the Administrator Access security objective, O.ADMIN, and also supports the Access Mediation security objective, O.ACCESS.

FIA_ADA.1 **Authorized Administrator, Trusted Host, and** User Authentication Data Initialization

181 This component is included to support the need to initialize authentication data and to manage it over time by an authorized administrator in support of O.ACCOUNT and O.ADMIN.

FIA_ADP.1 Basic **Authorized Administrator, Trusted Host, and** User Authentication Data Protection

182 This component is included to provide protection for user authentication data. Doing so is considered critical for satisfying security objectives, O.ACCOUNT and O.PROTECT.

FIA_AFL.1 Basic Authentication Failure Handling

183 This component is included to prevent repeated, undetected attempts to attack the firewall, especially attempts at guessing IDs and authentication data such as passwords. It directly supports O.PROTECT, and also supports the Administrator Access security objective, O.ADMIN, and the Individual Accountability security objective, O.ACCOUNT.

FIA_ATA.1 **Authorized Administrator, Trusted Host, Host, and** User Attribute Initialization

184 This component is included to support the Individual Accountability security objective, O.ACCOUNT, by supporting the need for user attributes to be defined and initialized.

FIA_ATD.2 Unique **Authorized Administrator, Trusted Host, Host, and** User Attribute Definition

185 This component is included to support the dependency identified in FPT_TSA.2. It supports the need to define the shared attributes and directly supports the Individual Accountability security objective, O.ACCOUNT.

FIA_UAU.1 Basic **Authorized Administrator** Authentication

186 This component requires the firewall administrator to always login before using the firewall. This component is included to provide direct support for the Individual Accountability security objective, O.ACCOUNT.

FIA_UAU.2 Single-use Authentication Mechanisms

187 This component is intended to require the firewall to support one-time passwords. This component is included to provide direct support for the Individual Accountability security objective, O.ACCOUNT.

FIA_UID.2 Unique Identification of **Authorized Administrators, Trusted Hosts, and Hosts**

188 This component is included to support the dependencies identified in FPT_TSA.2 and FAU_GEN.1 and to support the Individual Accountability security objective, O.ACCOUNT.

FCS_COP.2 Standards-Based Cryptographic Operation

189 This component is included to provide support for protecting the authorized administrator's dialogue with the firewall when the capability for remote administrator access is provided. This component directly supports the capabilities required under FPT_TSM.1, and the Firewall Self-Protection security objective, O.PROTECT.

FPT_RVM.1 Non-Bypassability of the TSP

190 This component is fundamental to the implementation of security products, and is included to require the firewall to mediate each and every request for services and

resources from network users. This is directly in support of O.PROTECT and indirectly supports O.ACCESS.

FPT_SEP.1 TSF Domain Separation

191 This component is included to ensure that the firewall itself is protected from attack by untrusted subjects. Because of this, this component has to be included to ensure the firewall can protect itself should it offer this additional functionality. This component supports the Firewall Self-Protection security objective, O.PROTECT.

FPT_TSA.2 Separate Security Administrative Role

192 This component is included to provide a means to administer the security functions of the firewall, and to control the exercise of administrative functions by supporting a distinct administrator role. This component is directly in support of the Administrator Access security objective, O.ADMIN.

FPT_TSM.1 Management Functions

193 This component further specifies the abilities necessary to successfully and securely administer the firewall. This component is directly in support of the Administrator Access security objective, O.ADMIN.

FAU_GEN.1 Audit Data Generation

194 This component is included to specify the particular types of audit events, as well as minimal content for the audit records, for PP-compliant firewalls. Note that only "failure" events need to be auditable in FAU_GEN.1.2.a, so the amount of information that is required should be manageable. This component directly supports the Auditing security objective, O.AUDIT.

FAU_MGT.1 Audit Trail Management

195 This component is included to further define the requisite audit trail management capabilities. This component directly supports the Auditing security objective, O.AUDIT.

FAU_POP.1 Human Understandable Format

196 Audit data are useless unless there is some means to view them; this component requires that they be viewable. This component directly supports the Auditing security objective, O.AUDIT.

FAU_PRO.1 Restricted Audit Trail Access

197 This component is included to restrict access to the review tools. This component directly supports the Auditing security objective, O.AUDIT, and the Administrator Access security objective, O.ADMIN.

FAU_SAR.1 Restricted Audit Review

198 This component requires that tools be available for viewing audit data, and that the use of these tools be restricted to the authorized administrator. This component directly supports the Auditing security objective, O.AUDIT, and the Administrator Access security objective, O.ADMIN.

FAU_SAR.3 Selectable Audit Review

199 This component specifies that a limited search and sort capability must be present; because of the volume of audit data, this requirement makes perfect sense. This component directly supports the Auditing security objective, O.AUDIT.

FAU_STG.3 Prevention of Audit Data Loss

200 This component not only satisfies dependencies generated by the audit reporting requirements, but also includes a limit as to the number of audit records lost due to both failure and attack; important to support the Auditing security objective, O.AUDIT, with respect to maintaining a relatively complete audit record.

	O.ACCESS	**O.ADMIN**	**O.ACCOUNT**	**O.PROTECT**	**O.AUDIT**
FDP_ACC.2	X				
FDP_ACF.4	X				
FDP_ACF.2	X				
FDP_RIP.3	X				
FDP_SAM.1	X	X			
FDP_SAQ.1	X	X			
FIA_ADA.1		X	X		
FIA_ADP.1			X	X	

Table 6.3 - Summary of Mappings Between Security Objectives and Functional Requirements

FIA_AFL1		X	X	X	
FIA_ATA.1			X		
FIA_ATD.2			X		
FIA_UAU.1			X		
FIA_UAU.2			X		
FIA_UID.2			X		
FCS_COP.2				X	
FPT_RVM.1	X			X	
FPT_SEP.1				X	
FPT_TSA.2		X			
FPT_TSM.1		X			
FAU_GEN.1					X
FAU_MGT.1					X
FAU_POP.1					X
FAU_PRO.1		X			X
FAU_SAR.1		X			X
FAU_SAR.3					X
FAU_STG.3					X

Table 6.3 - Summary of Mappings Between Security Objectives and Functional Requirements

6.4 RATIONALE FOR ASSURANCE REQUIREMENTS

201 EAL2 was chosen to provide a low to moderate level of independently assured security in the absence of ready availability of the complete development record from the vendor. As such, minimal additional tasks are imposed upon the vendor to the extent that if the vendor applies reasonable standards of care to the development, evaluation may be feasible without vendor involvement other than support for functional testing. The chosen assurance level should satisfy all functional dependencies, and is consistent with the postulated threat environment.

Specifically, that the threat of malicious attacks is not greater than moderate, and the product will have undergone a search for obvious flaws.

Appendix A

Vulnerability List for AVA_VLA.1

This appendix addresses service or application-related vulnerabilities. If the service described in one of the following vulnerabilities is not supported by the TOE, then the vulnerability is not applicable. The TOE shall also be subject to a search for obvious operating system and platform vulnerabilities.

FTP daemon vulnerabilities

Description:

In certain versions of the FTP daemon, a vulnerability exists allowing local and remote users to gain root privileges. This is accomplished through different means for distinct version such as through the signal handling routine increasing process privileges or through exploiting the SITE EXEC command.

See the relevant CERT advisory summaries including, CA-97:16, CA-95:16, and CA-94:08.

rlogin with TERM environment variable vulnerability

Description:

If, during an rlogin attempt on certain vulnerable systems, the buffer containing the value of the TERM environment variable is overflowed, arbitrary code can be executed as root.

See the relevant CERT advisory summaries including, CA-97:06.

Sendmail vulnerabilities

Description:

Remote users may be able to execute arbitrary commands with root privileges on systems receiving mail that are running a vulnerable version of sendmail that support MIME.

A second vulnerability to certain versions of sendmail occurs when an attacker gains group permissions of another user. This is possible when mail is sent to a users .forward or :include: file which is located in a directory that is writable by the attacker.

A third vulnerability to certain versions of sendmail occurs when users other than root invoke sendmail in daemon mode, bypassing code intended to prevent this.

A fourth vulnerability to certain versions of sendmail occurs when buffer overflows lead to unauthorized users gaining root access.

A fifth vulnerability to certain versions of sendmail occurs in the case of resource starvation. A user with an account can exploit sendmail when sendmail cannot distinguish between a “resource failure” and “user id not found” error. Starving sendmail will create files owned by the “default user” which can then be used to gain access to other files owned by that user.

See the relevant CERT advisory summaries including, CA-97:05, CA-96:25, CA-96:24, CA-96:20, and CA-95:08.

Telnet Environment Option vulnerability

Description:

If the system to which the Telnet connection attempt is directed is running Telnet daemons that are RFC 1408 or RFC 1572 compliant and the system supports shared object libraries then the system may be vulnerable. Both users with and without accounts on the system could become root by transferring environment variables that influence the login program called by the Telnet daemon.

See the relevant CERT advisory summaries including, CA-95:14.

TFTP daemon attacks

Description:

Remote users on the Internet may access world-readable files on an internal network using an unrestricted TFTP service. Thus sensitive files could be retrieved by an adversary on the external side of the firewall.

See the relevant CERT advisory summaries including, CA-91:19 and CA-91:18.

Syslog Vulnerability

The syslog(3) subroutine uses an internal buffer for building messages that are sent to the syslogd(8) daemon. This subroutine does no range checking on data stored in this buffer. It is possible to overflow the internal buffer and rewrite the subroutine call stack. It is then possible to execute arbitrary programs.

This problem is present in virtually all versions of the UNIX Operating System except the following:

- Sony's NEWS-OS 6.X
- SunOS 5.5 (Solaris 2.5)
- Linux with libc version 4.7.2 released in May, 1995

The sendmail(8) program uses the syslog(3) subroutine, and a script has been written and is being used to exploit the vulnerability.

Impact: Local and remote users can execute commands. Prior access to the system is not needed. Exploitation can lead to root access.

See the relevant CERT advisory summaries including, CA-95:13.

IP Spoofing attacks

Description:

Firewalls are vulnerable to IP spoofing attacks, including TCP SYN Flooding attacks. Firewalls should have a mechanism to handle SYN Flooding attacks. Firewalls should be capable of preventing traffic from entering the protected local network when packets claim to originate from local network, broadcast network, reserved network, or loopback network addresses.

See the relevant CERT advisory summaries including, CA-96:21.

UDP attacks

Description:

Tools exist to flood UDP ports with packets causing degradation in system performance and increased network congestion. Firewalls must be capable of being configured to filter all UDP services.

See the relevant CERT advisory summaries including, CA-96:01.

ICMP (ping) vulnerability

Large ICMP datagrams may cause systems to crash, freeze, or reboot, resulting in a denial of service.

See the relevant CERT advisory summaries for more information including, CA-96.26.

IP loose source route option vulnerability

Description:

Firewalls should be capable of rejecting packets that use the IP loose source route option. A TCP connection where the loose source route option is enabled allows an attacker to explicitly route packets through the network to a destination without following the usual routing process. A malicious attacker can pose as a host that is on the return path for this type of TCP traffic since, according to RFC 1122, the traffic must follow the reverse order of the route which it followed from source to destination.

RIP vulnerability

Description:

As a result of the ease with which bogus RIP packets may be injected into a network, packets can be lead away from their intended destination if the attacking host is closer to the target than the valid sending host. This occurs when routers accept RIP packets and because RIP performs no type of authentication. Firewalls should be configured to disallow routing along certain links such as intermediate links on an external network while the source and destination hosts are both on the internal network.

ARP vulnerability

Description:

Because any host can respond to an ARP request, a malicious host can send false ARP responses back to the sender before the true recipient receives the ARP request and responds back. Thus the sender will now be fooled into sending traffic to the malicious host in the middle rather than the proper destination host. The malicious host can either impersonate the destination host, or intercept, modify, and resend the traffic to the sending host's intended destination. Firewalls should not allow ARP requests to pass through them and should not perform proxy ARP for requests from an external network.

DNS vulnerabilities

Description:

A flood of DNS responses injected into the network could cause a denial of service since the DNS server may become confused.

A DNS resolver may check several different levels before checking the correct one. If a host, FOO.BAR.COM, attempts to connect to ONE.TWO, the check will be made first to ONE.TWO.BAR.COM and then to ONE.TWO.COM and finally to ONE.TWO. Thus a malicious host can impersonate a domain that the resolver would encounter before encountering the appropriate level.

If an attacker can contaminate a target's DNS responses cache before the call is made, the target can be fooled into believing that the cross-check it performs is legitimate. As a result, the attacker gains access.

References

[1] *Common Criteria for Information Technology Security Evaluation*, CCEB-96/011, Version 1, dated 96/01/31.

[2] *US Government Application Gateway Firewall for Low Risk Environments*; Version 1.0, December 1997.

[3] Federal Information Processing Standard Publication (FIPS-PUB) 140-1, *Security Requirements for Cryptographic Modules*, dated January 11, 1994

[4] Federal Information Processing Standard Publication (FIPS-PUB) 46-2, *Data Encryption Standard (DES)*, December 1993.

[5] Federal Information Processing Standard Publication (FIPS-PUB) 81, *DES Modes of Operation*, December 1980

Acronyms

The following abbreviations from the Common Criteria are used in this Protection Profile:

CC	Common Criteria for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IT	Information Technology
POP	Post Office Protocol
PP	Protection Profile
rlogin	Remote Login
SFP	Security Function Policy
ST	Security Target
SNMP	Simple Network Management Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

Addendum

CERT Advisory Vulnerability Summaries

The following are vulnerabilities derived from the CERT advisories.

CA-97:16 — ftpd Signal Handling Vulnerability

The signal handling routine causes this vulnerability by increasing a remote users' process privileges to root, while continuing to catch other signals. This creates a race condition allowing anonymous as well as regular FTP users to gain root access. This allows users to read or write arbitrary files to the server.

CA-97:06 — rlogin with TERM environment variable Vulnerability

Many implementations of the rlogin program contain a defect whereby the value of the TERM environment variable is copied to an internal buffer inappropriately. The buffer holding the copied value of TERM can be overflowed. In some implementations, the buffer is a local variable, meaning that the subroutine call stack can be overwritten and arbitrary code executed. The arbitrary code executed is under the control of the user running the rlogin program.

Since the rlogin program is set-user-id to root in order for it to have the server allocate a port in the range of 0-1023, this programming defect can be exploited to execute arbitrary code as root.

CA-97:05 — MIME Conversion Buffer Overflow in Sendmail vers 8.8.3 and 8.8.4 Vulnerability

Sendmail can be configured on a mailer-by-mailer basis for either 7-bit ASCII or 8-bit MIME according to flags set defined by the mailer. MIME conversion of email is usually done on final delivery.

Sending carefully crafted email messages to a system running either version 8.8.3 or 8.8.4 of sendmail, intruders may be able to force sendmail to execute arbitrary commands as root. Intruders can do this without having an account.

The restricted shell program of sendmail should be used with all versions of sendmail. Using this gives you improved administrative control over the programs that sendmail executes on behalf of users.

If you run /bin/mail based on BSD 4.3 UNIX, replace /bin/mail with mail.local, which is included in the sendmail distribution. As of Solaris 2.5 and beyond, mail.local is included in the standard distribution.

Although the current version of mail.local is not the perfect solution to sendmail problems, it does counter known vulnerabilities that are being exploited. For more details, see CA-95:02.

Leaving executable copies of older versions of sendmail installed elsewhere (such as in /usr/lib), allows vulnerabilities in those versions to be exploited if an intruder gains access to your system. Either delete these versions or change the protections on them to be non-executable.

Similarly, if you replace /bin/mail with mail.local, remember to remove old copies of /bin/mail or make them non-executable.

CA-96:26 — Denial of Service attack via ping

The TCP/IP specification allows for a maximum packet size of up to 65536 octets. It is known that some systems will react in an unpredictable fashion, including crashing, freezing, and rebooting, when receiving oversized IP packets.

In particular, Internet Control Message Protocol (ICMP) ECHO_REQUEST and ECHO_RESPONSE messages, used by a local host to determine whether a system is reachable via the network, issued via the ping program have been used to trigger this behavior.

The firewall shall be able to handle oversized ICMP datagrams without resulting in a denial of service.

CA-96:25 — Version 8 Sendmail Group Permissions Vulnerability

When version 8 of sendmail causes mail to be delivered to a program listed in .forward or :include:, that program is run with the group permissions possessed by the user owning that .forward or :include: file.

It is possible for users to obtain group permissions they should not have by linking to a file that is owned by someone else, but on which they have group write permissions. By changing that file, users can acquire group permissions of the owner of that file.

Exploitation is possible if the attacked user has a file that is group writable by the attacker on the same file system as either the attacker's home directory, or an :include: file that is referenced directly from the aliases file and is in a directory writable by the attacker. The first .forward attack works only against root. This attack does not give users root "owner" permissions, but does give them access to the groups that list root in /etc/group.

CA-96:24 — Sendmail daemon mode vulnerability

Sendmail is often run in daemon mode so that it can "listen" for incoming mail connections on the standard SMTP port. The root user is the only user allowed to start sendmail in this way, and sendmail contains code intended to enforce this restriction.

Sendmail can be invoked in daemon mode bypassing the built-in check. When the check is bypassed, any local user can start sendmail in daemon mode. And as of version 8.7, sendmail will restart itself after receiving a SIGHUP signal. It will re-execute itself as root, using the

exec system call. Thus, by manipulating the sendmail environment, the intruder can then have sendmail execute an arbitrary program as root.

CA-96:21 — TCP SYN Flooding and IP Spoofing Denial of Service Attacks

The firewall shall be thoroughly examined to see how it handles TCP SYN Flooding attacks. This occurs when there are too many half-open connections (the server has sent a SYN-ACK and is waiting for the client to send an ACK back to the server). When the data structure available for handling pending connections fills up with too many pending connections, all new connection attempts will be refused. Normally, there is a timeout associated with a pending connection, however the attacker can just send connection requests faster than the server can clear the expired half-open connections in the structure.

IP Spoofing Attacks

Though these cannot be stopped entirely, the firewall must be capable of being set up to restrict packets to the external interface by not allowing a packet through if it has a source address from the internal network(s). In addition, the firewall shall be capable of recognizing and filtering outgoing packets that have a source address different from the internal network(s) to prevent source IP address spoofing from originating on the internal network.

The firewall's input filter should also be capable of filtering packets that come from Broadcast Networks (both the all 0's and all 1's broadcast networks), and these private reserved networks: 127.0.0.0 - 127.255.255.255 (loopback) 10.0.0.0 - 10.255.255.255 (reserved) 172.16.0.0 - 172.31.255.255 (reserved) 192.168.0.0 - 192.168.255.255 (reserved)

Turning off IP source routing, though recommended, will not stop IP spoofing attacks.

CA-96:20 — 2 Sendmail Vulnerabilities up to and including version 8.7.5

Buffer Overflows

There are several buffer overflows present in Sendmail version 8.7.5 and earlier. Some of the buffer overflows could result in local users gaining unauthorized root access. This must be prevented.

Resource Starvation

Anyone with access to an account on the system can run programs or write files as the default user. The danger of compromising the default user depends primarily on the other files in your system owned by that user.

CA-96:01 — UDP port Denial of Service Attack

Hacker programs exist to cause "UDP Packet Storms." When the packet storm is directed at a single host this causes the host's performance to degrade. When the packet storm is between two hosts this causes not only each host's performance to degrade, but also causes extreme network congestion. For example, by connecting a host's chargen service to the echo service

on the same or different machine, the effected machine(s) perform(s) poorly.

The firewall shall be capable of filtering UDP services, especially chargen and echo. All UDP ports less than 900 shall be capable of being filtered. We recommend that the firewall filter all unused UDP services.

CA-95:16 — Improper configuration of the SITE EXEC FTP daemon command

Certain configurations of the SITE EXEC command in the systems FTP server are vulnerable to attack. The problem is that the variable _PATH_EXECPATH was set to "/bin" in the configuration file, when it should be set to "/bin/ftp-exec" or some similar directory that does not contain a shell or command interpreter. Only a user with a local account on such an improperly configured system offering the FTP service may gain root access.

CA-95:14 — Telnetd Environment Option Vulnerability

If the remote or targeted system where a Telnet is connecting runs an RFC 1408 or RFC 1572 compliant Telnet daemon and the targeted system also supports shared object libraries, then it may be vulnerable to attack. It may be possible to transfer environment variables that influence the login program called by the Telnet daemon. A user may then bypass the normal login and authentication scheme and may become root on that system.

Thus if such a Telnet daemon is vulnerable, it should be replaced with one that changes the environment given to the login program.

CA-95:13 — Syslog Vulnerability

The syslog(3) subroutine uses an internal buffer for building messages that are sent to the syslogd(8) daemon. This subroutine does no range checking on data stored in this buffer. It is possible to overflow the internal buffer and rewrite the subroutine call stack. It is then possible for local and remote users to execute arbitrary programs. Several programs use the syslog subroutine including, Sendmail, httpd, ftpd, and telnetd. All these and other programs that use syslog are vulnerable to this problem.

CA-95:08 — Sendmail Version 5 Vulnerability

Users of Version 5 sendmail that have not upgraded are vulnerable. Local and remote users can create files, append to existing files or run programs on the system. Exploitation of this vulnerability can lead to root access.

CA-94:08 — ftpd SITE EXEC Vulnerability

Some implementations of ftpd that support the SITE EXEC command feature of the ftpd daemon are vulnerable in that a local or remote user can gain root access. The SITE EXEC

feature must be explicitly activated in order to be exploited. There is also a race condition in certain implementations that also leads to root access.

CA-91:19 — IBM AIX TFTP Daemon Vulnerability

Unrestricted TFTP access allows remote sites to retrieve copies of any world-readable files. Use of unrestricted TFTP would allow anyone on the Internet to retrieve copies of a sites sensitive files such as /etc/passwd. The intruder could later crack the password file and use the information to login to accounts. This may provide root access.

The TFTP protocol should be filterable by the firewall or a file writable only by root (such as /etc/tftpaccess.ctl) shall exist on systems on the inside network to restrict the files that should be accessible. Firewalls configured to allow TFTP access shall make the possible dangers of its use clear in the documentation.

CA-91:18 — TFTP Internet attacks Vulnerability

Unrestricted TFTP access allows remote sites to retrieve a copy of any world-readable file.

Anyone on the Internet can use TFTP to retrieve copies of a site's sensitive files. For example, the recent incident involved retrieving /etc/passwd. The intruder can later crack the password file and use the information to login to the accounts. This method may provide access to the root account.

Sites that do not need TFTP should disable it immediately by editing the system configuration file to comment out, or remove, the line for tftpd. This file may be /etc/inetd.conf, /etc/servers, or another file depending on your operating system. To cause the change to be effective, it will be necessary to restart inetd or force inetd to read the updated configuration file.